



MAC OSX User Manual

Version 1.1

Welcome to nCrypteCloud!

nCrypteCloud is a Privacy, Security, and Collaboration application that uses Industry Standard Encryption Technology (AES-256 bit encryption) to secure files stored in the cloud.

Through seamless cloud integration, nCrypteCloud acts as a layer on top of cloud storage services, giving you the ability to apply additional security features to your existing cloud data.

The policies you apply to your cloud data remain consistent no matter where the data travels, how the data is accessed, or what actions are performed on the data, allowing you to stay in full control of your cloud content.

This user guide will show you how to use nCrypteCloud to securely store, share, and collaborate on the cloud.

Welcome to nCryptedCloud!	2
Getting Started 1	4
How to Create a Dropbox Account	4
How to Install Dropbox	4
How to Register and Sign into Dropbox	5
How To Install nCryptedCloud	6
How To Register For nCryptedCloud	10
Identities 2	13
How to Add a Corporate Identity	13
How to Select Your Identity	15
Make Private 3	16
How To Make Private	16
How To Remove Privacy	18
Trusted Sharing 4	19
Desktop Client	20
Web Portal	23
Share Securely 5	25
How To Share Securely	25
How to View "Shared With"	27
How to Manage Folder Membership	29
How to Revoke Access	30
Auditing 6	31
How to Access Personal Auditing Page	31
Sensitivity 7	32
How To Apply Sensitivity	32
Pin Lock 8	34
How to set a centralized Pin	34
How to enable PIN Lock on the nCrypted Cloud Client	35
Multiple Cloud Provider/Custom Folders 9	38
How to set up nCrypted Cloud with Google Drive and SkyDrive (OneDrive)	39
How to Set Up nCrypted Cloud with Box and Egnyte	41
How to add local directories to your nCrypted Cloud folder	42
Icon Glossary	44

Getting Started

1

Install and Create A Dropbox Account

In order to use nCrypteCloud, you must have a Dropbox account. If you do not have a Dropbox Account, please follow the instructions below to create one.

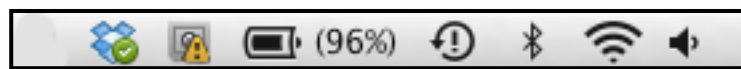
How to Create a Dropbox Account

1. Go to (https://www.dropbox.com/login?lhs_type=anywhere)
2. Enter your Name, Email, and Password to create an account
3. You will be redirected to the Dropbox Install page

Now that you have a Dropbox account, follow these steps to install Dropbox onto your computer.

How to Install Dropbox

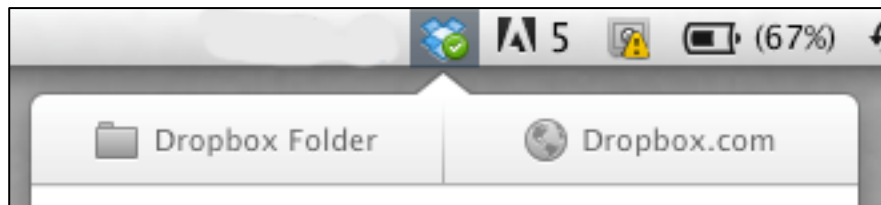
1. Go to the Dropbox Install Website (<https://www.dropbox.com/install>) if you were not already re-directed there and click "Free Download"
2. Click on the .dmg file that you just downloaded to run the Dropbox Installer
3. Double-click on the Dropbox icon to install
4. The Dropbox icon will appear in your menu bar



Now that you have just successfully downloaded Dropbox, you can continue through the registration process.

How to Register and Sign into Dropbox

1. Open Dropbox by double clicking the Dropbox icon in your menu bar
2. A pop up window will appear-- select "I already have a Dropbox account"
3. Sign in using the email and password you just set up, verify your computer name, and click Continue
4. Choose your desired Dropbox Plan (2GB: free, 00gb \$10/month; 200gb: \$20/month) and click continue
5. Choose Typical or Advanced Setup, then Click Install
6. If you would like to Install Dropbox on your mobile phone, enter your mobile number and click Continue
7. Continue through the Dropbox Tour and click Finish



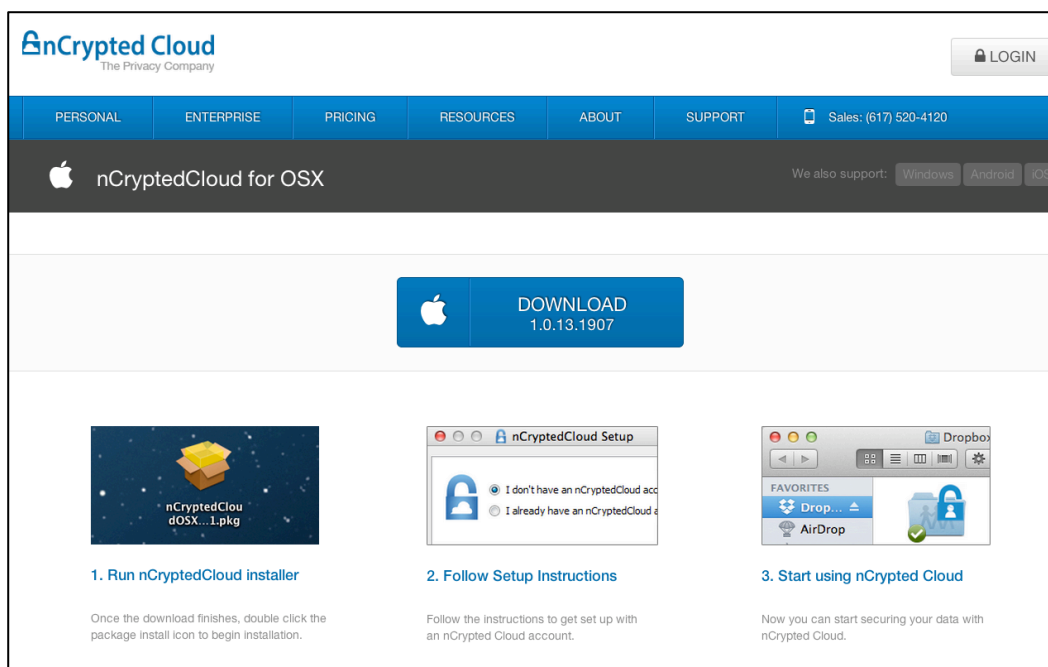
Confirm that Dropbox is installed by right-clicking the Dropbox icon

Now that you have registered for a Dropbox account and installed the software, you can now download and register for nCrypteCloud by following these instructions.

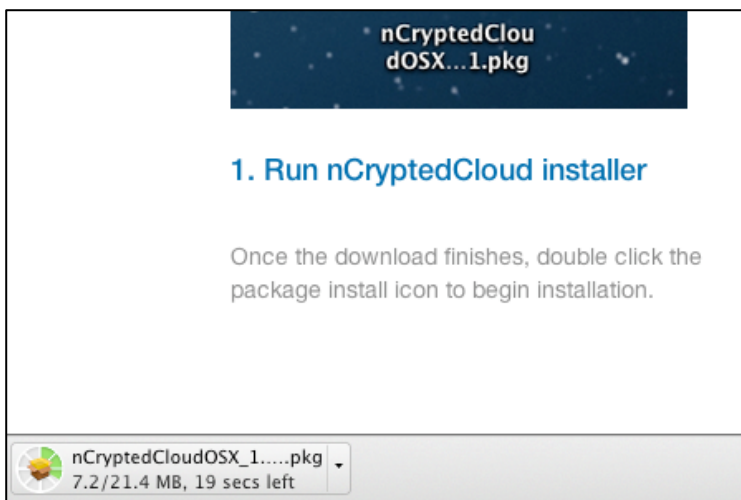
Install and Register for nCrypteCloud

How To Install nCrypteCloud

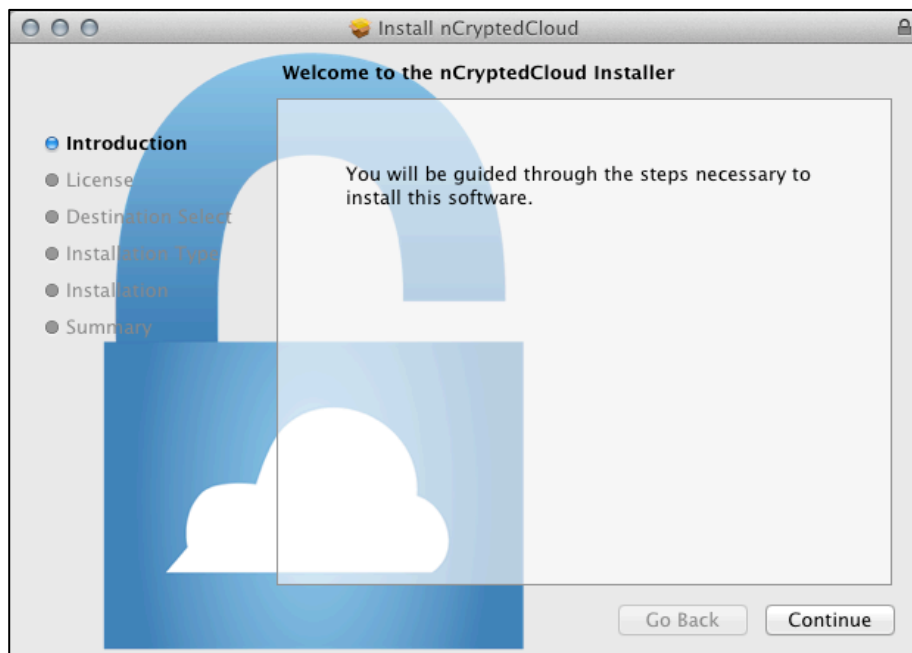
1. Go to the nCrypteCloud Download Page: <https://www.ncryptedcloud.com/download/>



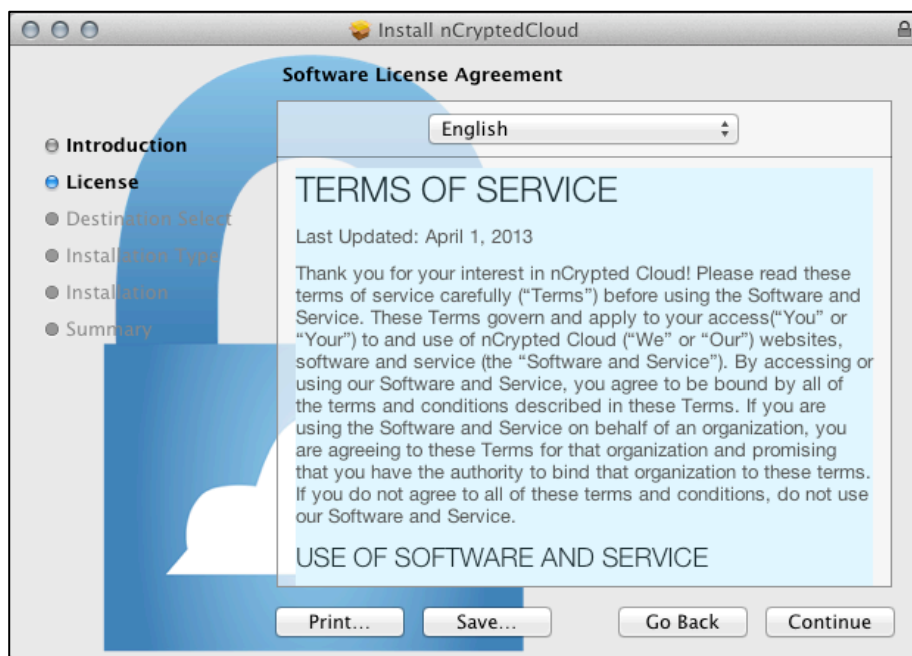
2. Click "Download" and nCrypteCloud's Install Package will begin downloading.



Once nCrypteCloud's Install Package is fully downloaded, double-click the file and begin the installation process.



3. Agree to nCrypteCloud's Terms of Service



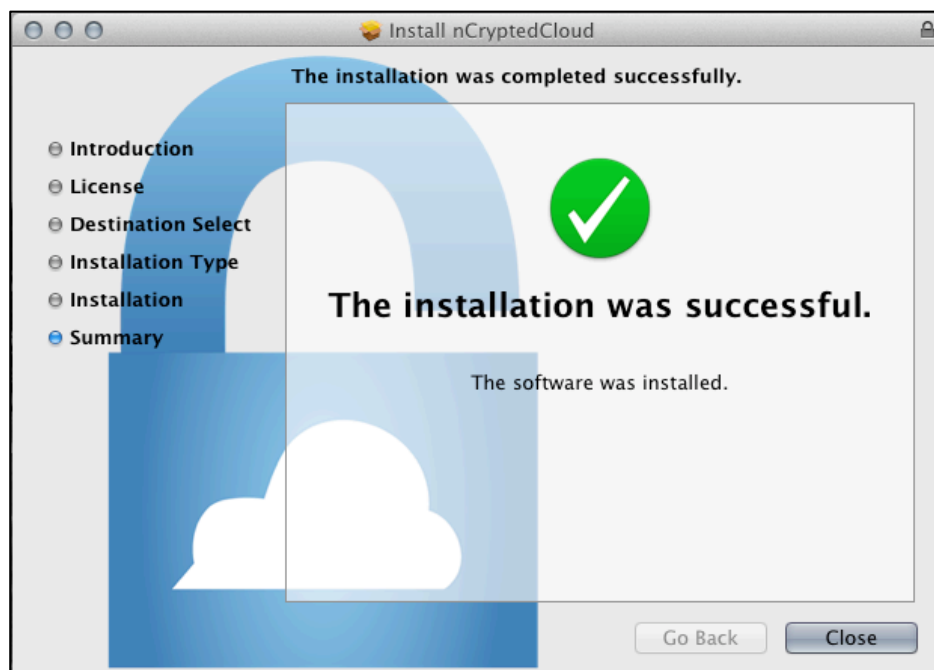
4. Choose an Install Destination



5. Sign in and select "Install Software"



nCrypteCloud will begin installing

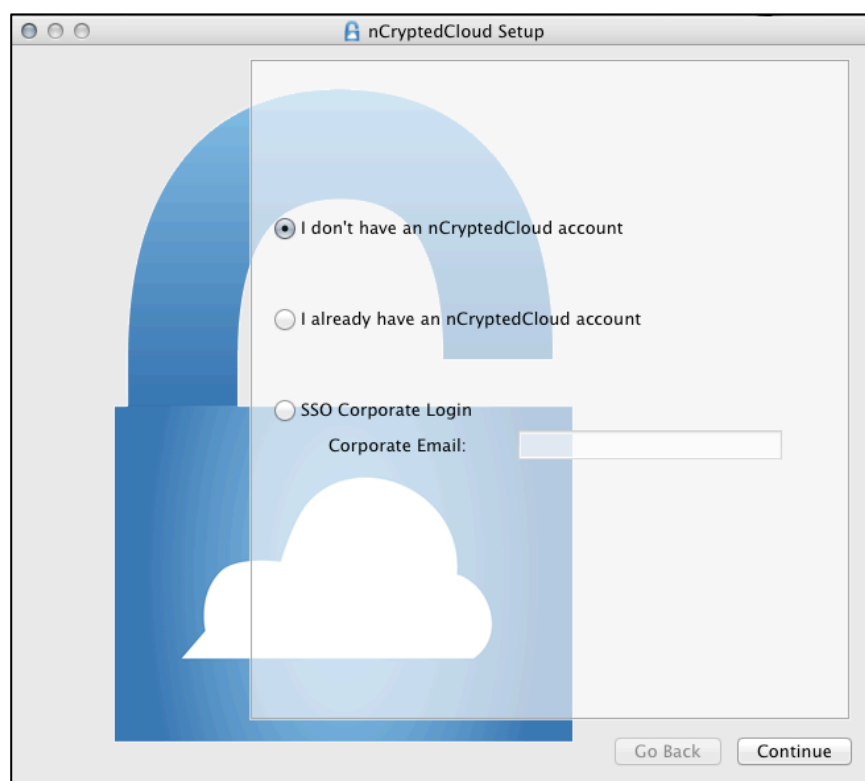


Congratulations! You have just successfully installed nCrypteCloud!

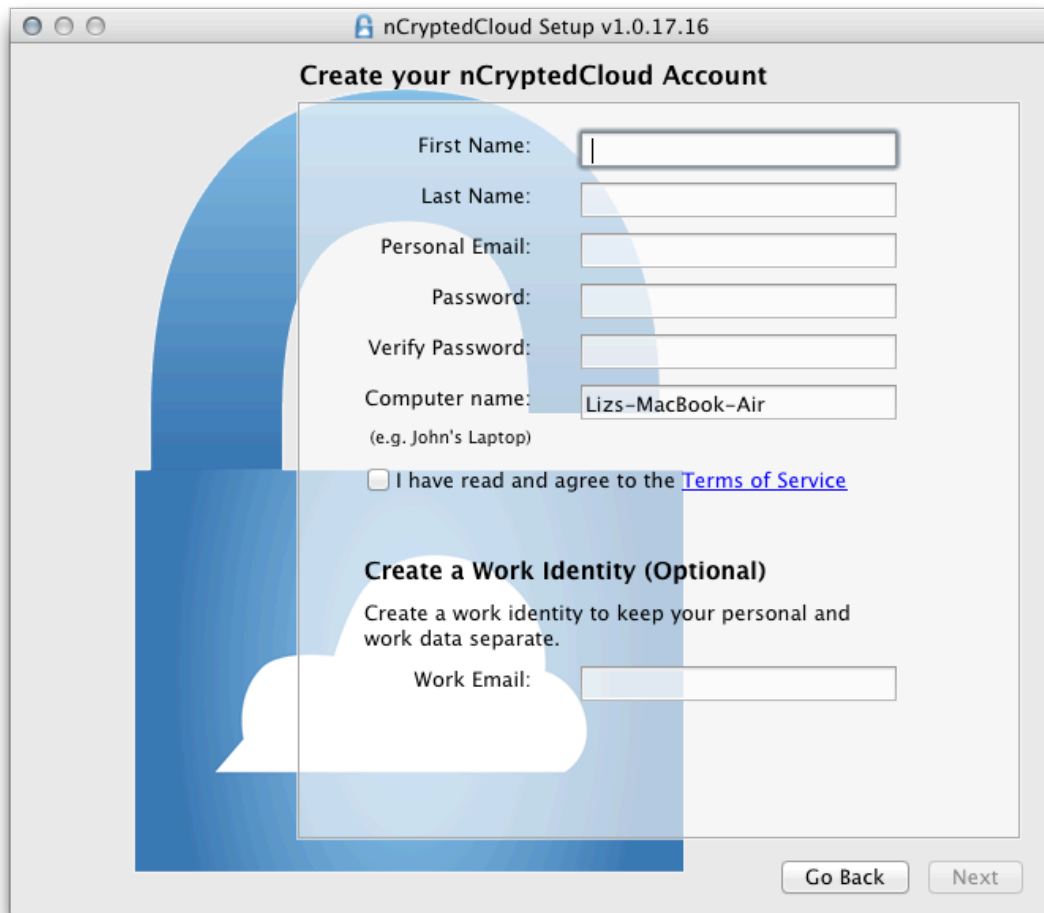
How To Register For nCrypteCloud

Now that you have successfully installed nCrypteCloud, you will be directed to a registration page. By registering for nCrypteCloud, you will have access to all of its features and capabilities.

1. Select "I don't have an nCrypteCloud account" to create an account.



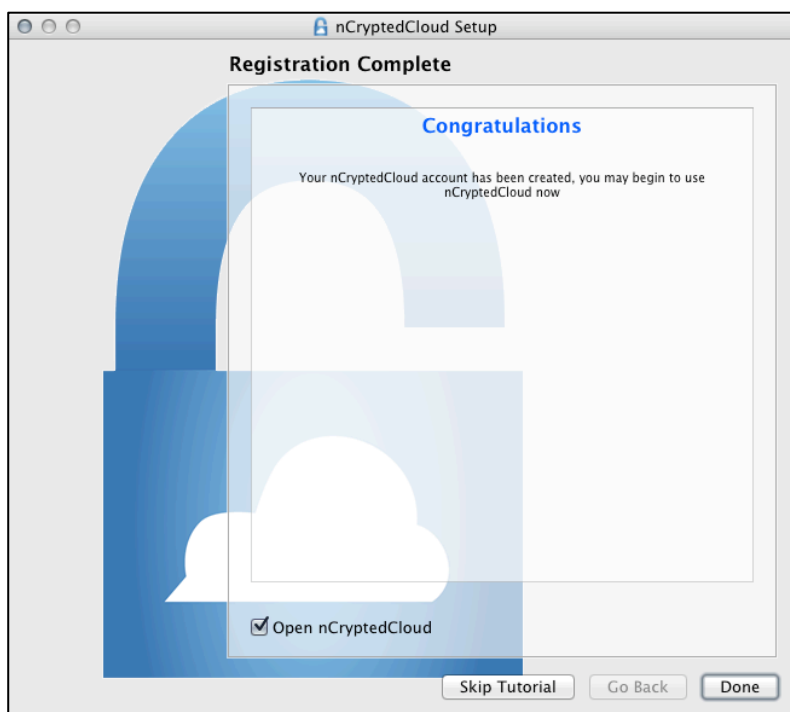
2. You will be asked to enter your name, personal email address, and chosen password.
(See following page)



The image shows a screenshot of the nCrypteCloud Setup v1.0.17.16 window. The window has a title bar with standard Mac OS window controls (red, yellow, green buttons) and the text "nCrypteCloud Setup v1.0.17.16". The main content area is titled "Create your nCrypteCloud Account". It contains several input fields: "First Name:", "Last Name:", "Personal Email:", "Password:", "Verify Password:", and "Computer name:". The "Computer name" field is pre-filled with "Lizs-MacBook-Air" and has a small note below it: "(e.g. John's Laptop)". Below these fields is a checkbox labeled "I have read and agree to the" followed by a blue hyperlink "Terms of Service". Underneath this is a section titled "Create a Work Identity (Optional)" with the text "Create a work identity to keep your personal and work data separate." and a "Work Email:" input field. At the bottom right of the window are two buttons: "Go Back" and "Next". A large, semi-transparent blue cloud graphic is visible in the background of the form area.

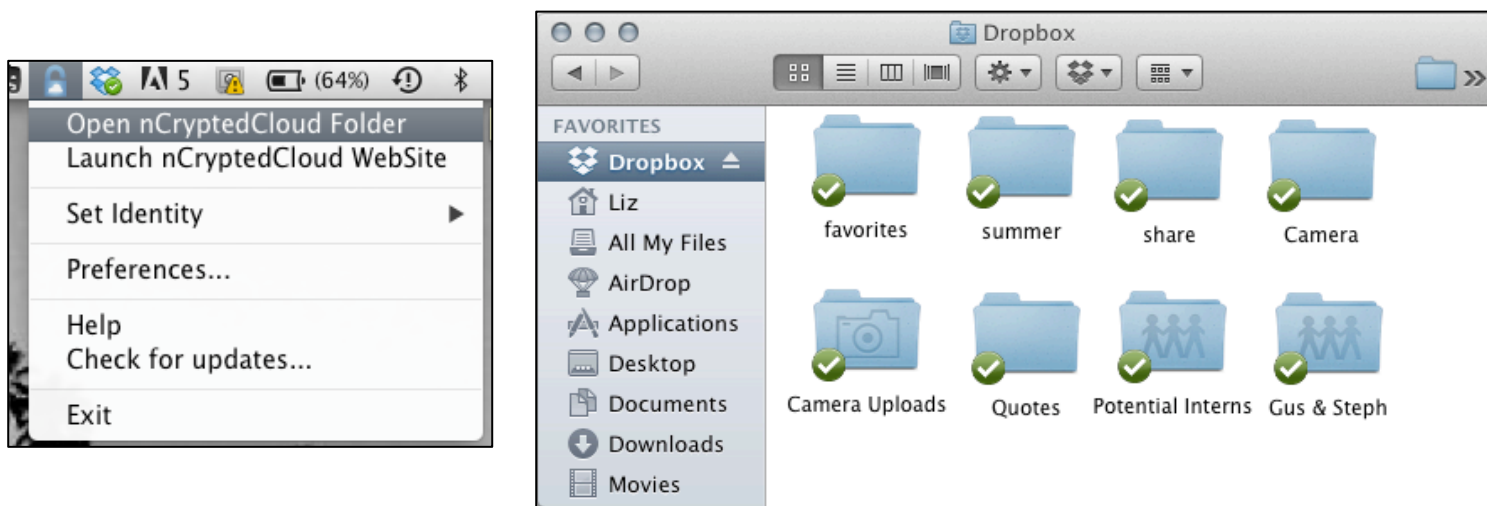
If you wish to create a work identity, you have the option to do so at the bottom of the screen. If you enter a work email address in the 'Personal Email' section (line 3), nCrypteCloud will automatically detect that you are using a corporate email and enter your corporate email address for you in the 'Work Email' section.

After you fill out all the designated sections, agree to the Terms of Service and click "Next



The screen above confirms that you have just successfully registered for nCrypteCloud!

To access nCrypteCloud, click on the blue lock icon in your menu bar and select "Open nCrypteCloud Folder". This will open your Dropbox folder.



Identities

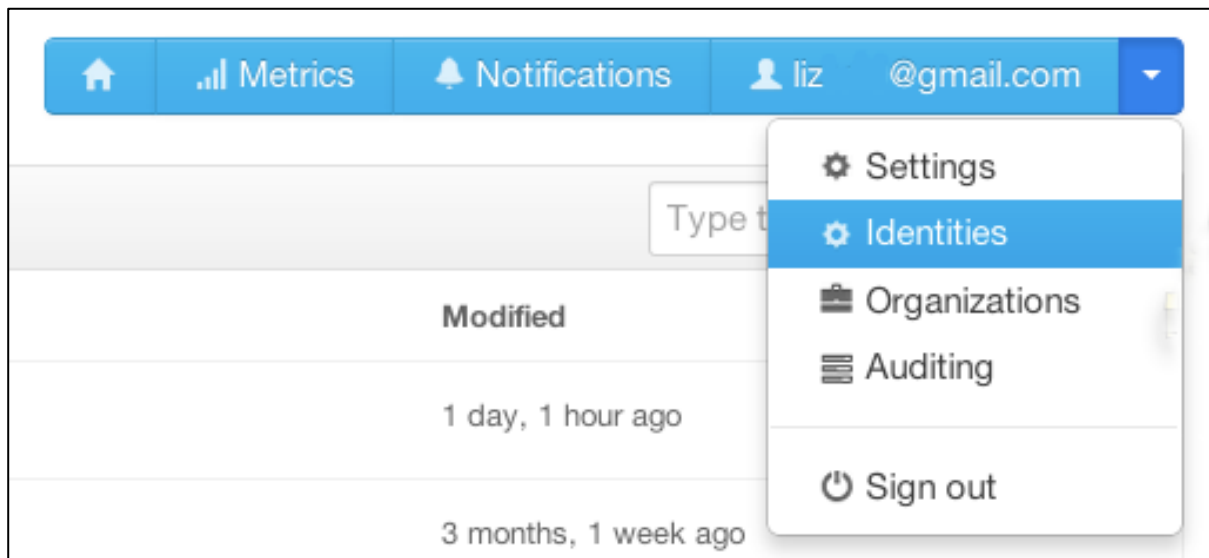
2

You have one personal and potentially many corporate identities with which you can manage and collaborate. By managing your identities, you can keep personal data separate from corporate data within the same cloud.

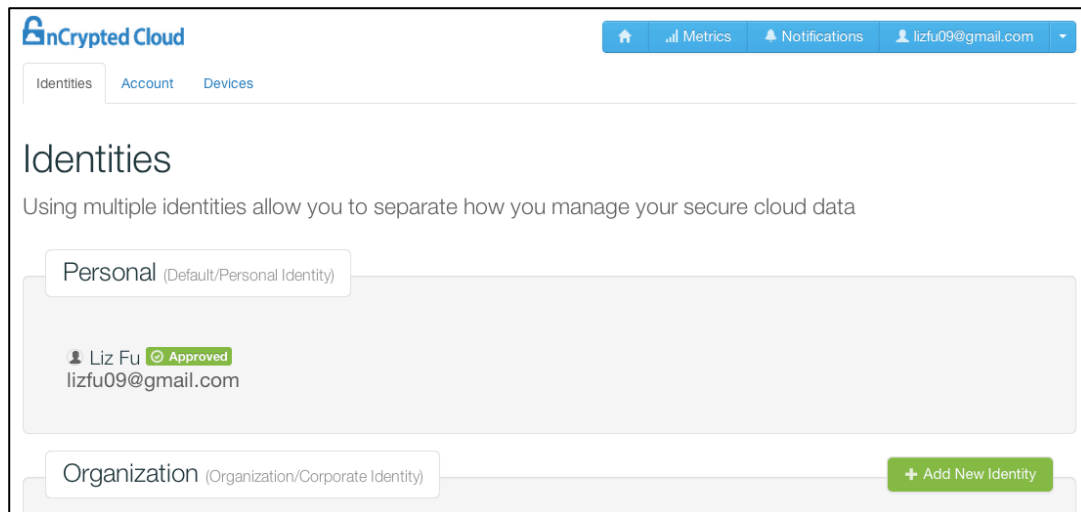
If you did not already create a work identity during the registration process, follow the steps below to do so.

How to Add a Corporate Identity

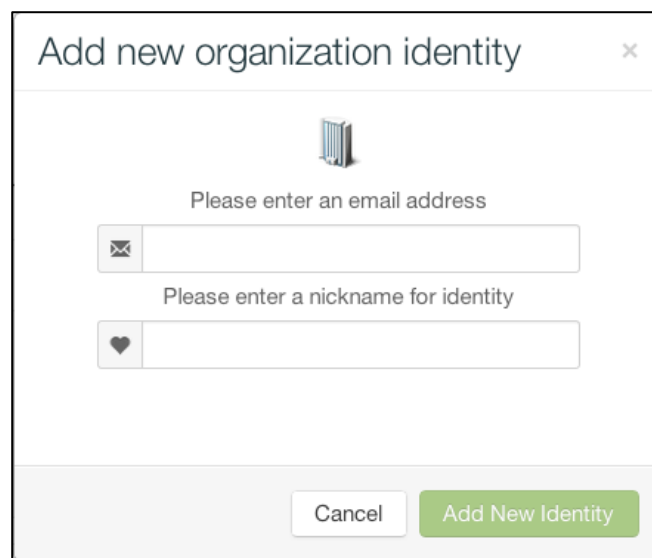
1. Log into your nCryptedCloud account on the nCryptedCloud web portal
2. Click on your arrow next to your username at the top right corner of the page. Select "Identities"



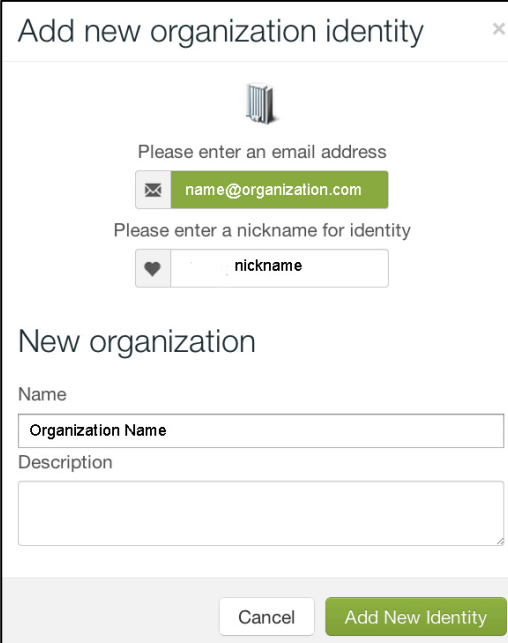
3. You will be redirected to your Identities page. Click "Add New Identity", located below your 'Personal' section and right above the 'Organization' section.



4. A dialog box will appear and you will be asked to enter a new email address and an identity nickname.



5. nCrypteCloud will detect that your email is connected to an organization. If the organization is already approved, you will receive an email from nCrypteCloud to verify your email address.

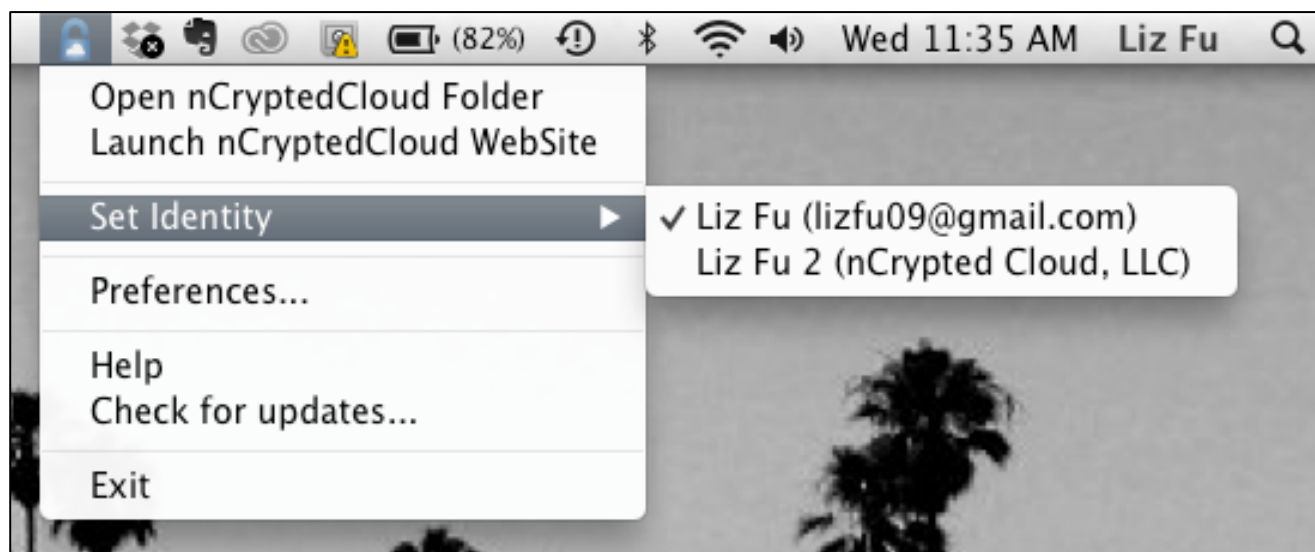


A dialog box titled "Add new organization identity" with a close button (X) in the top right corner. It contains two input sections: "Please enter an email address" with a green button labeled "name@organization.com", and "Please enter a nickname for identity" with a text field labeled "nickname". Below these is a section titled "New organization" with a "Name" label and a text field labeled "Organization Name", and a "Description" label with a larger text area. At the bottom are "Cancel" and "Add New Identity" buttons.

If nCrypteCloud does not recognize the organization, you will be asked to enter the information for the organization.

How to Select Your Identity

1. Right click on the nCrypteCloud desktop icon and select "Set Identity"
2. Select the identity you would like to operate as

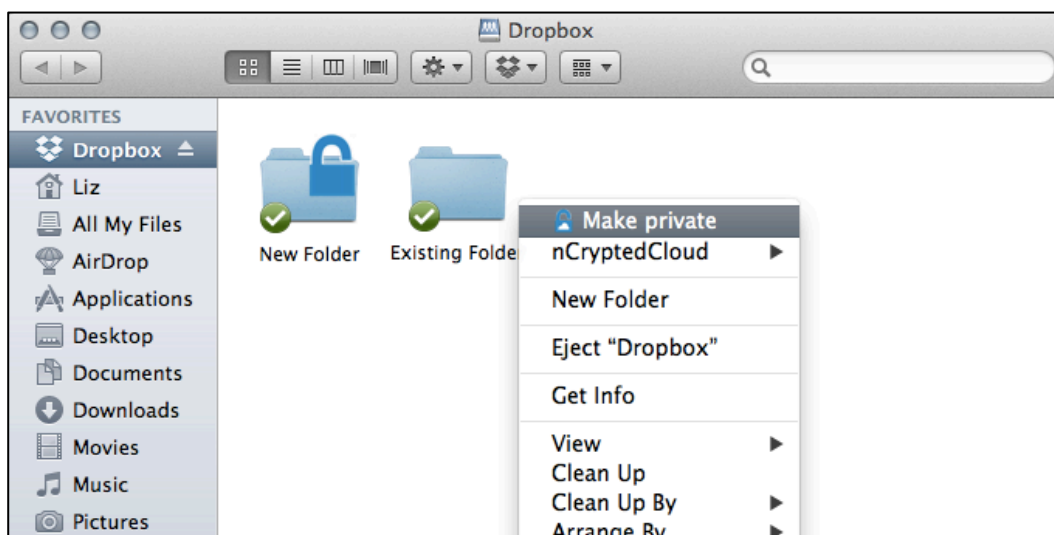


Make Private

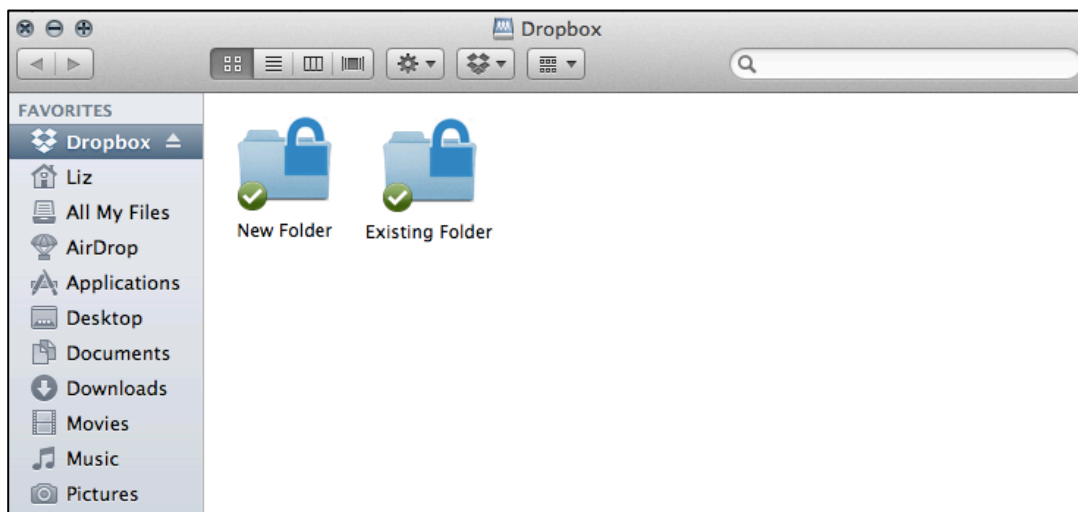
3

How To Make Private

To make an existing folder private, simply right click the folder and select 'Make Private'.



A blue lock icon will appear on the top right corner of that folder.



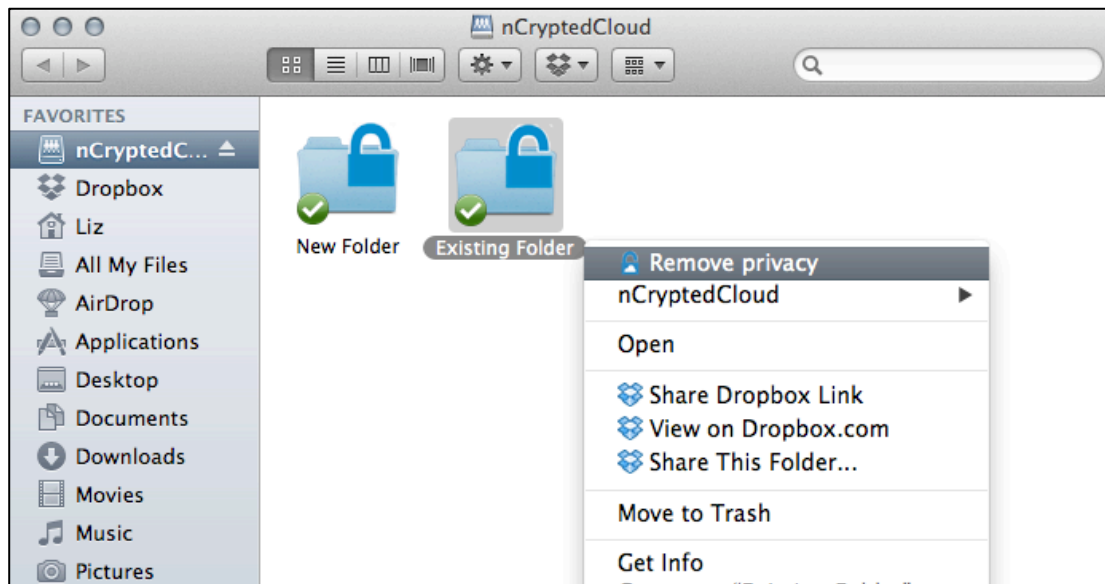
If you choose your 'Personal' identity, all folders you encrypt become 'Personal' folders and will appear with a blue lock icon as seen below (left).



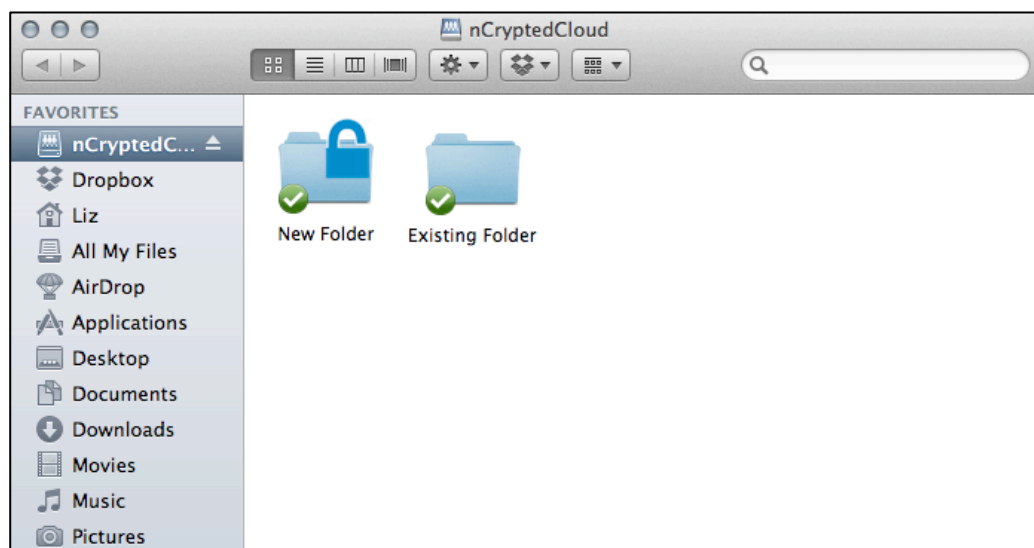
If you choose your 'Corporate' identity, all folders you encrypt become 'Corporate' folders and will appear with a briefcase icon as seen above (right).

How To Remove Privacy

To remove privacy, simply right click and select "Remove Privacy"



The blue lock icon will no longer be at the top right corner of the folder, indicating that it is no longer private and encrypted.



Trusted Sharing

4

nCrypteCloud's Trusted Sharing Feature allows you to share encrypted files or entire directories with anyone on a one-off basis through nCrypteCloud's Desktop Client, Mobile Application, and Web Portal. With Trusted Sharing, you can control the duration of time your file/s is being shared for as well as how it can be viewed. Additionally, nCrypteCloud gives you the option to watermark your file/s, add a message, and require a security code to access them.

Expiration Timer: The expiration timer setting determines how long the recipient can view your file for. You can adjust the timer to expire after a certain number of days, hours, minutes, and seconds. You also have the option to set the expiration timer to 'never expire'.

Permissions: You can choose between three file permissions- Read Only, Download Only, and Read and Download. These three settings determine how the recipient can view the file/s.

Security Code: You have the option to require a security code to access your file/s. The recipient will receive two emails: one with the trusted sharing file, and a separate email with the security code enclosed. In order to access the data, the recipient must enter the security code when prompted. This added security feature ensures that your shared file/s do not fall into the wrong hands.

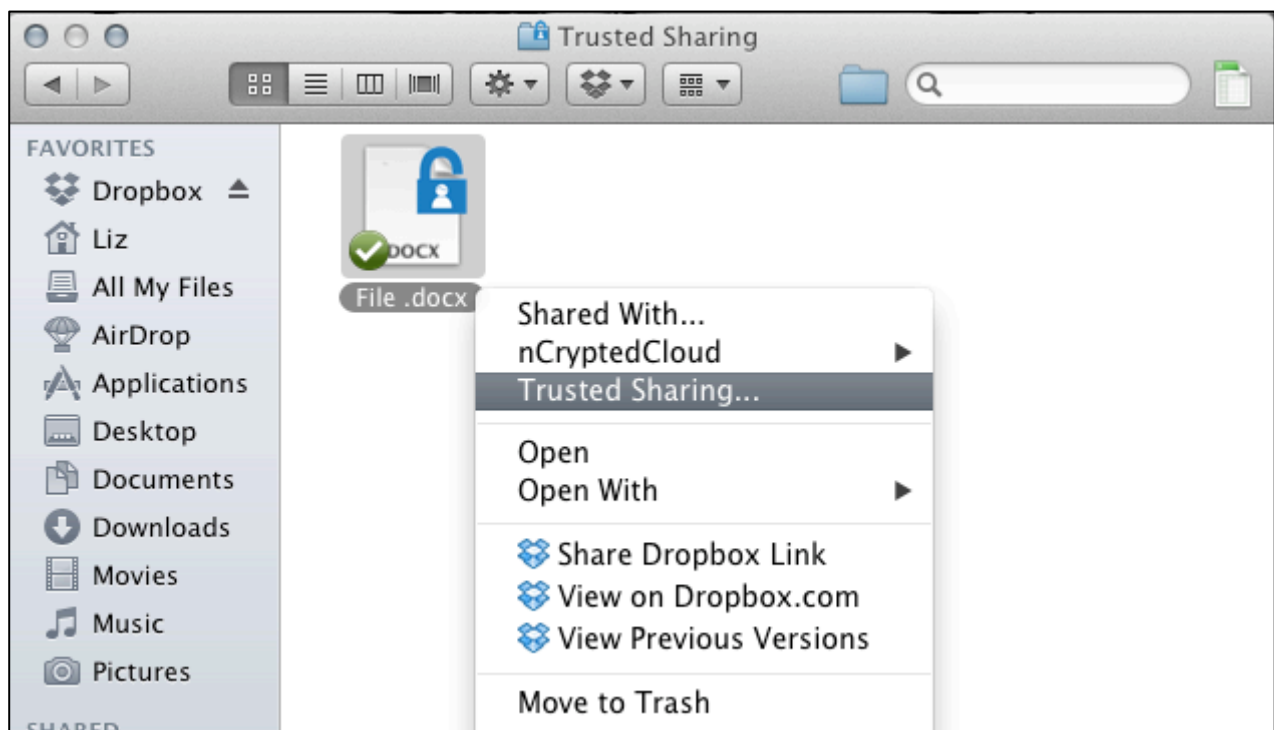
Watermark: nCrypteCloud gives you the option to watermark your file/s with the recipient's personal information (email, IP) to discourage sharing misconduct. If your data is

ever shared without your authorization, you will know exactly who was responsible for the misconduct.

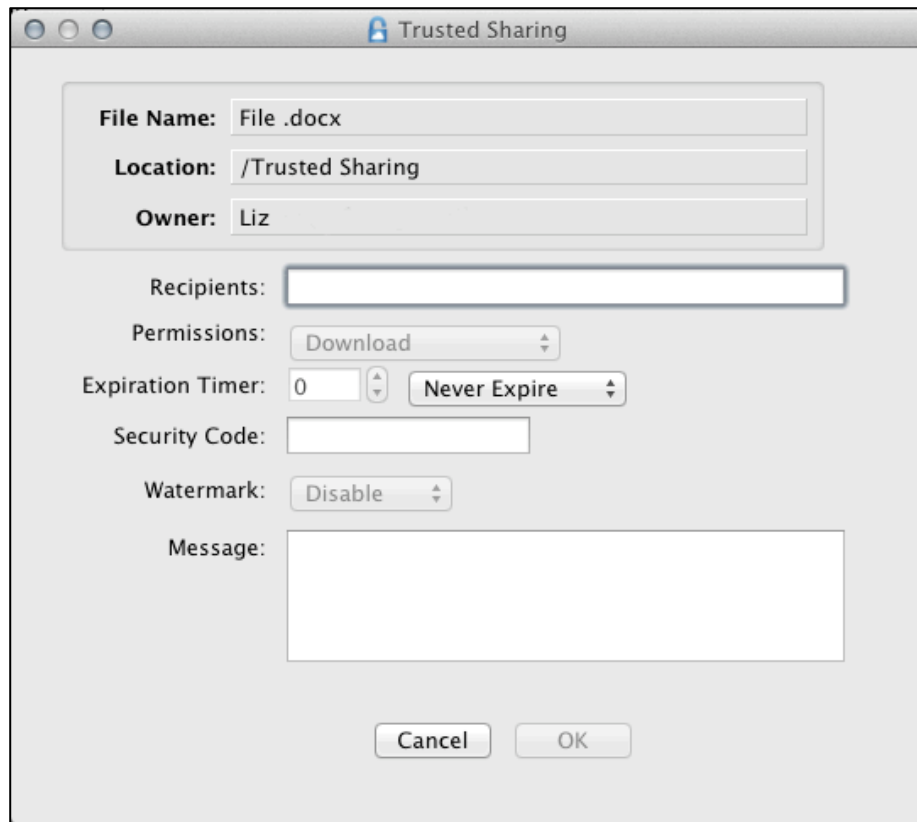
Desktop Client

To share a file or folder using Trusted Sharing on nCrypteCloud's Desktop Client

1. Right-click the file or folder you wish to share using "Trusted Sharing".



A pop-up window will appear.



2. Enter the email addresses belonging to the people you wish to share the file with under the 'Recipients' section.
3. Select the duration of time you wish to share the file for under the 'Expiration Timer' section.
4. Under the 'Security Code' section, you have the option to choose a security code that must be entered in order to access the file. This security code will be sent to the recipient in a separate email.
5. You have the option to watermark the file with the recipient's information to discourage misuse of information.
6. You also have the option to send a message with your trusted sharing file.

After clicking "OK", an email will be sent to the recipient with a link to your file. The email will look like the one pictured below:

Liz <no-reply@ncryptedcloud.com> [Details](#)

Liz securely shared File .docx with you via nCrypteCloud
September 10, 2013 2:31 PM

Greetings,

Liz securely shared "File .docx" with you using nCrypteCloud.
You can access this file by visiting: <https://www.ncryptedcloud.com/secure-sharing/231161DB-1212-4287-B96B-84A3DA8F7D65/>.

TRUSTED SHARING

Sincerely,

nCrypte Cloud Team
<http://ncryptedcloud.com>

If you required a security code, this is the separate email the recipient will receive:

Liz <no-reply@ncryptedcloud.com> [Details](#)

Here is your PIN to access secured file: File .docx
September 10, 2013 2:31 PM

Greetings,

Liz has securely shared "File .docx" with you using nCrypteCloud.
Here is the PIN to access this file: 1234 .

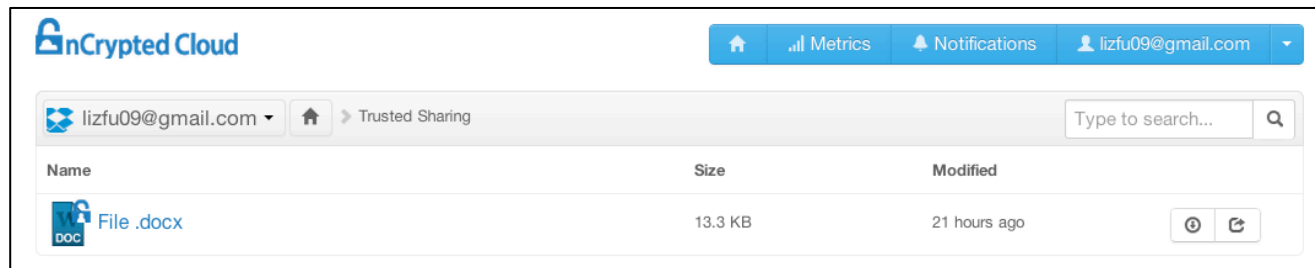
Sincerely,

nCrypte Cloud Team
<http://ncryptedcloud.com>

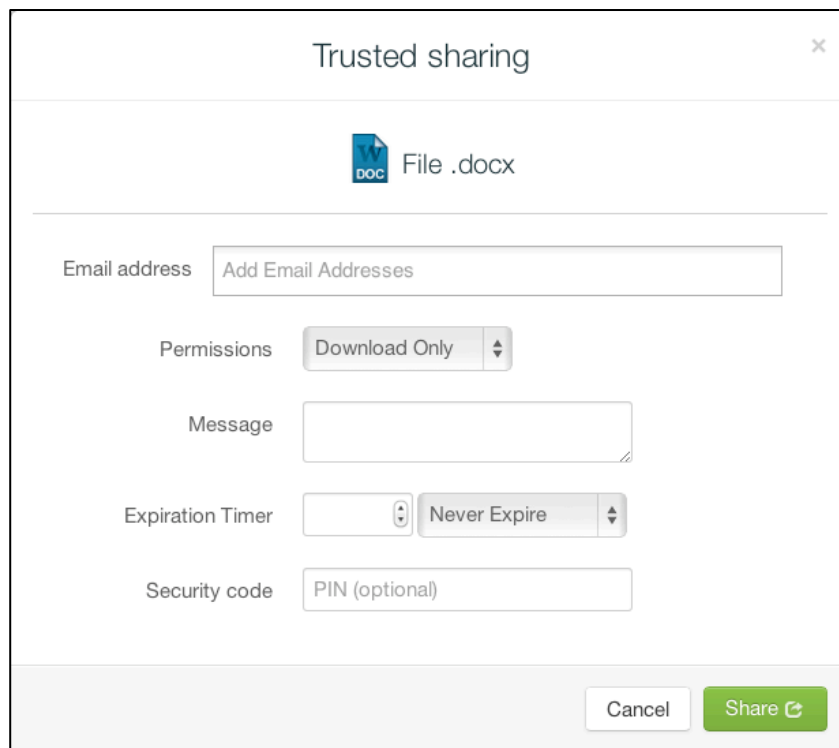
Web Portal

To send a file or folder via Trusted Sharing through nCrypteCloud's Web Portal, begin by going to <https://ncryptedcloud.com/> and signing into your account.

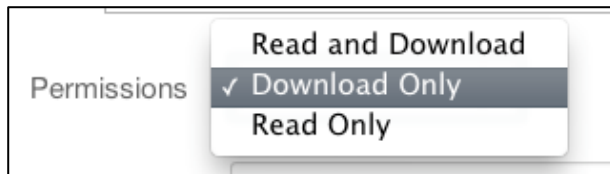
1. Choose the file or folder you want to share and click the arrow button that is located to the far right of your file/folder.



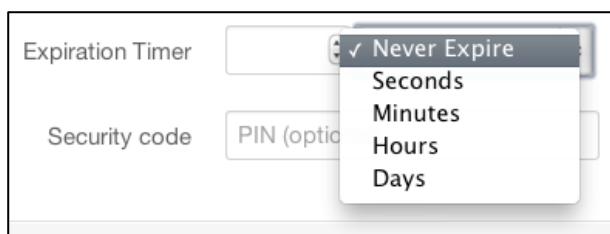
2. A pop-up window will appear. Enter the email addresses for the people you wish to share the file with.



3. You can choose between 3 permissions: Read and Download, Download Only, and Read Only. By default, the permission is set to 'Download Only'

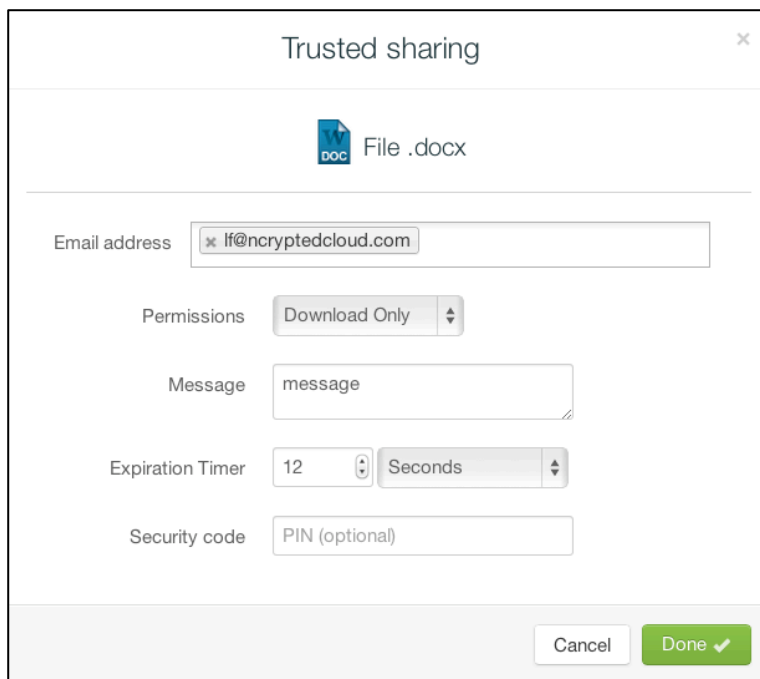


4. Select the amount of time you wish to share the file for.



5. Enter a security code and message if you wish, then click "Share"

To confirm that your file/folder was successfully shared via Trusted Sharing, the "Share" button will turn into a "Done" button.



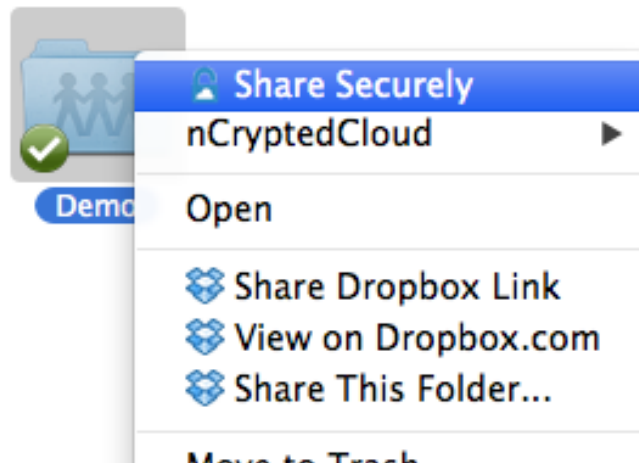
Share Securely

5

The Share Securely feature ensures that your cloud data is protected wherever it travels. The policies you set for your cloud data will remain with your data no matter who you share that data with, what device is used to access that data, and what actions are performed on the data.

How To Share Securely

1. Right click the folder you want shared securely and select "Share Securely"



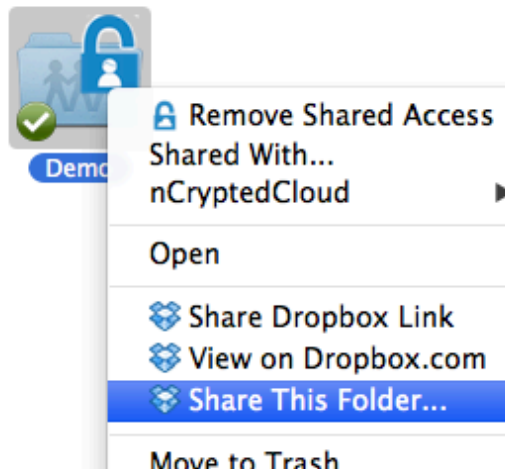
2. A blue lock icon with a silhouette of a person will appear on the folder and all the files within.



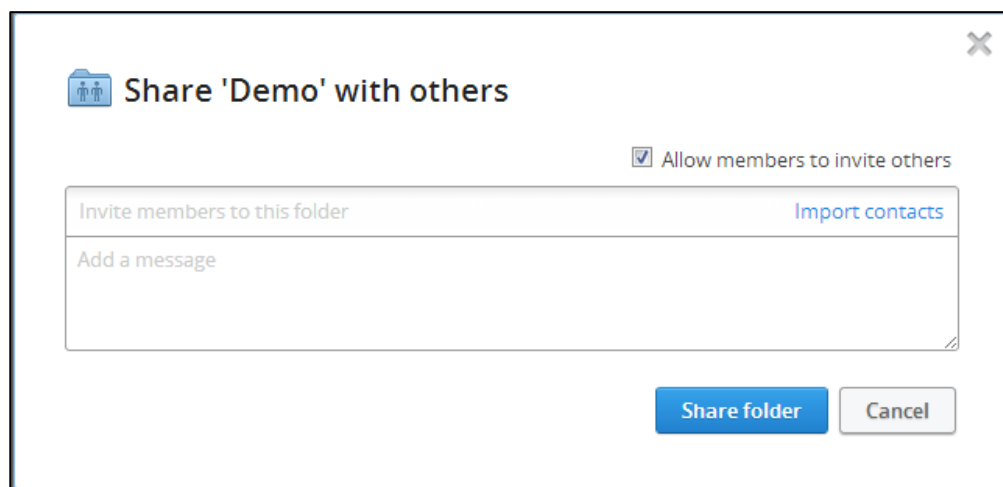
This icon signifies that the folder can be shared.

You can do the same for any additional folders you wish to create.

3. To share this folder, right click and select "Share This Folder." You will be redirected to the Dropbox page.



4. Enter the email addresses belonging to the people you would like to share the folder with and click "Share Folder".

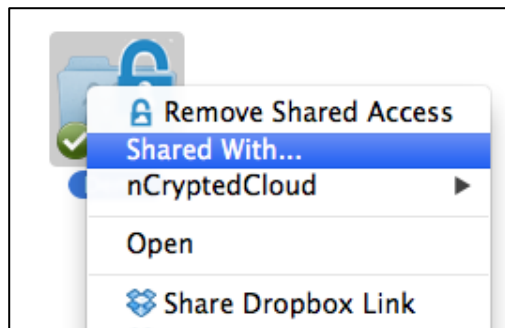


The recipients of the shared folder will receive a Dropbox and email notification to join this shared folder.

How to View “Shared With”

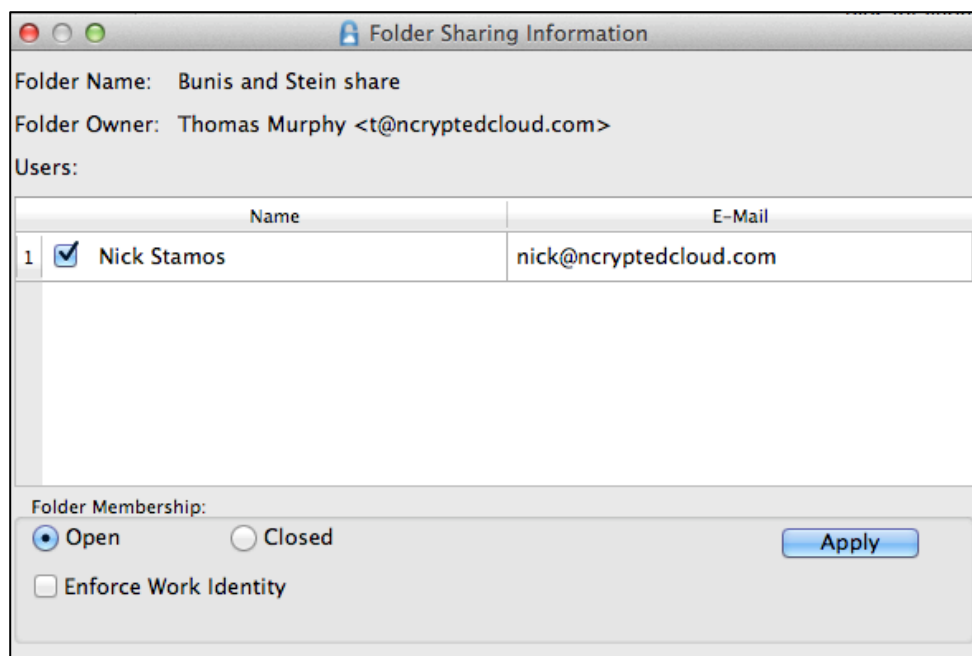
After you’ve shared a folder, it’s easy to keep track the people with whom it was shared.

1. Right click the shared folder and select “Shared With” from the drop-down menu

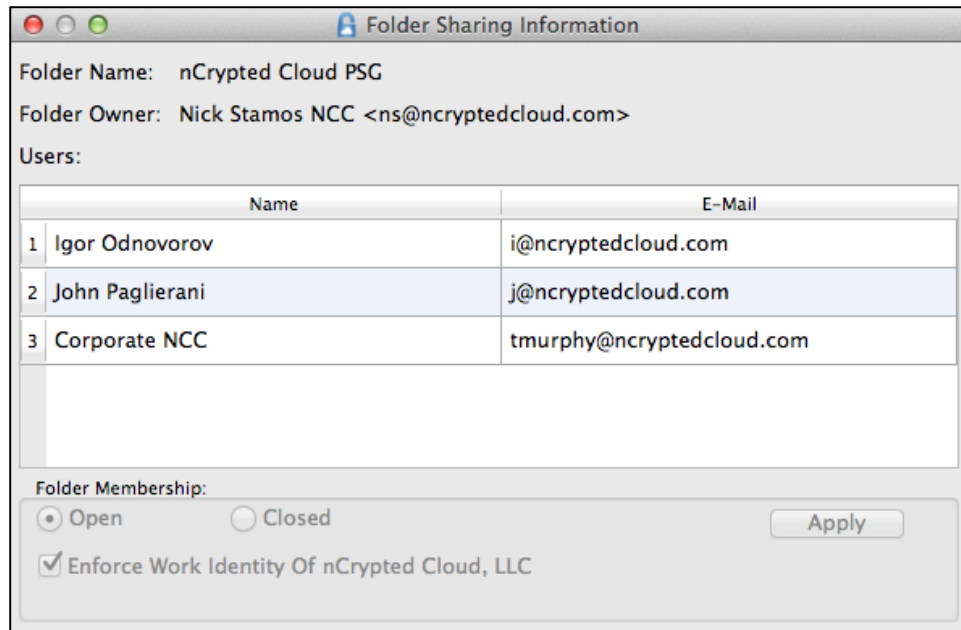


2. A dialogue box will appear with a list of all the people with whom the folder is shared

The image below is the dialogue box you, the **Folder Owner**, will see.



The image below is the dialogue box that the **recipients** of the shared folder will see.



As you can see, you are the only one who is able to change “Folder Membership.” This means that only you can control who can and cannot access this folder.

How to Manage Folder Membership

The Folder Owner can manage the "Folder Membership" by following these steps:

1. In the bottom of the Folder Sharing Information dialogue box you will see "Folder Membership"



2. You have the option to make the folder "Open" or "Closed," and to "Enforce Work Identity."

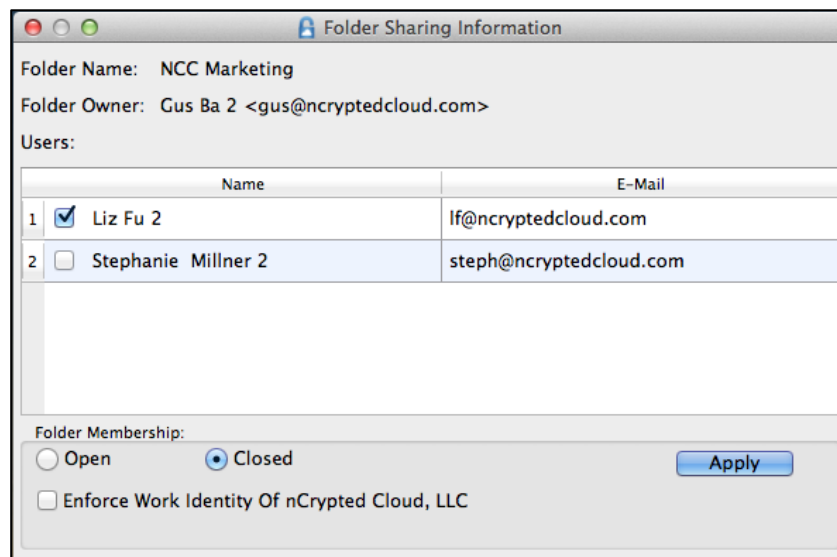
If you choose to leave the folder "Open," anyone that receives the link to the folder has access to the folder.

If you choose to make the folder "Closed," only the people listed as "Users" in the Folder Sharing Information dialogue box will have access to the folder.

How to Revoke Access

You can revoke access to the data belonging to this folder at anytime. This feature is extremely useful when a collaborator leaves a collaboration group, or an employee leaves a company. To revoke access, follow the steps below:

1. Check the box to the left of the user's name who you wish to remove. name of the user
2. Under "Folder Membership", select "Closed"
3. Click "Apply"



This function takes away the user's ability to access the data on all platforms. nCrypteCloud will refuse access to this data even if the data has been burned the data onto a CD, emailed the data, or put the data on a memory stick.

If this function was performed by accident, the owner can simply change the "Folder Membership" back to "Open" and click the "Apply" button. The selected user would then be able to access the information once again.

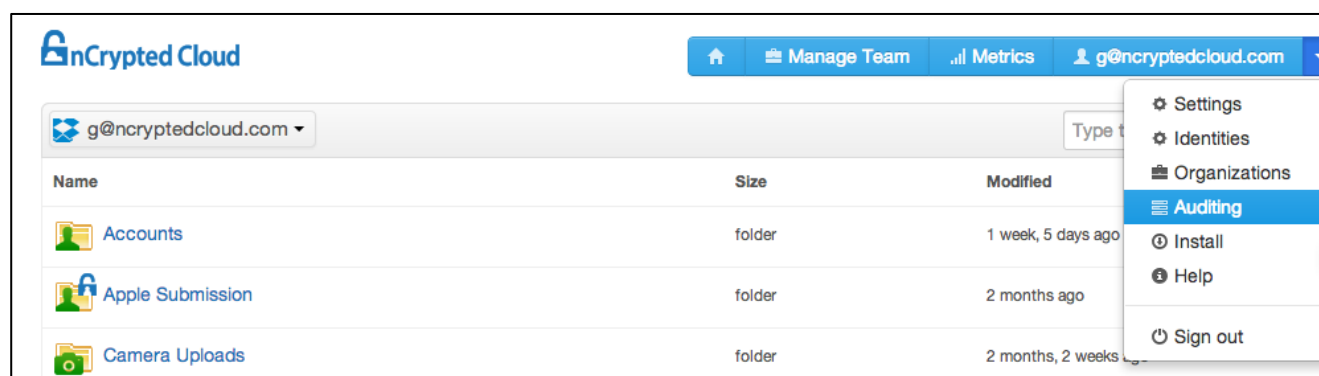
Auditing

6

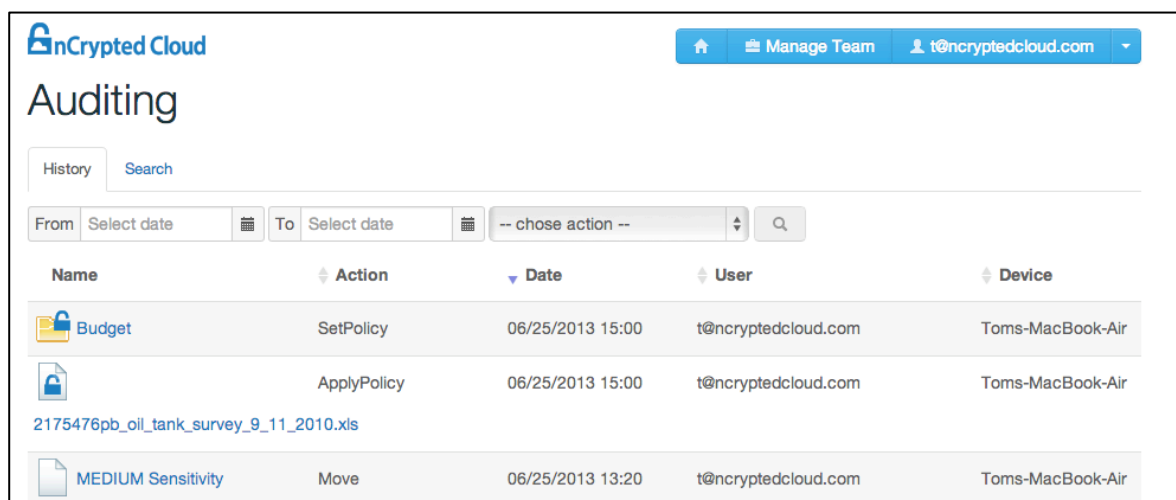
nCrypteCloud's Auditing feature gives you full forensic auditing of all access activities. This means you have the ability to see who accessed your data, when your data was accessed, from what device the data was accessed, and what actions were performed on your data.

How to Access Personal Auditing Page

1. Login to your nCrypteCloud account at www.ncryptedcloud.com
2. Click on the arrow icon in the top-right corner.
3. Click on "Auditing" from the drop-down list.



You will be directed to the auditing page.



Sensitivity

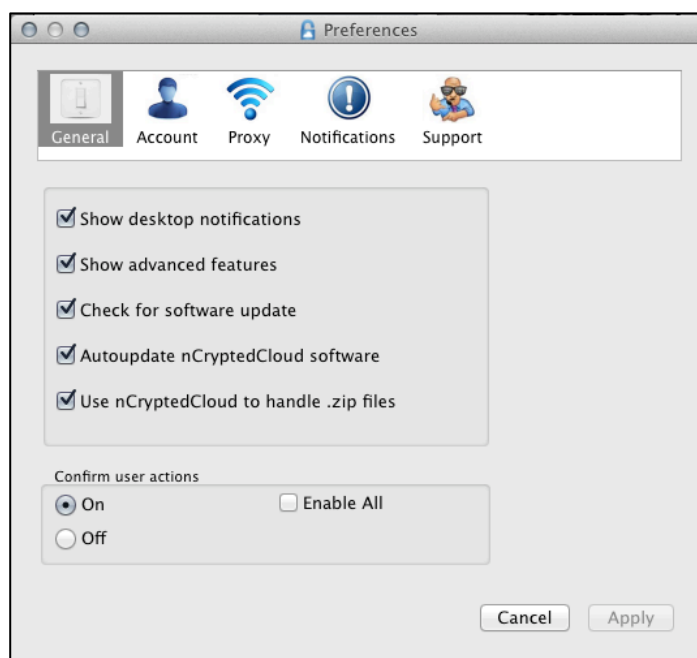
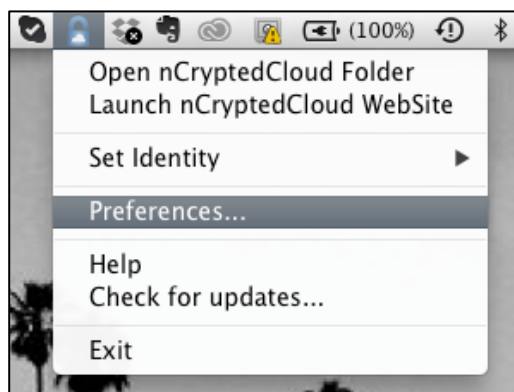
7

Sensitivity settings give you the ability to easily sort folders based on levels of importance.

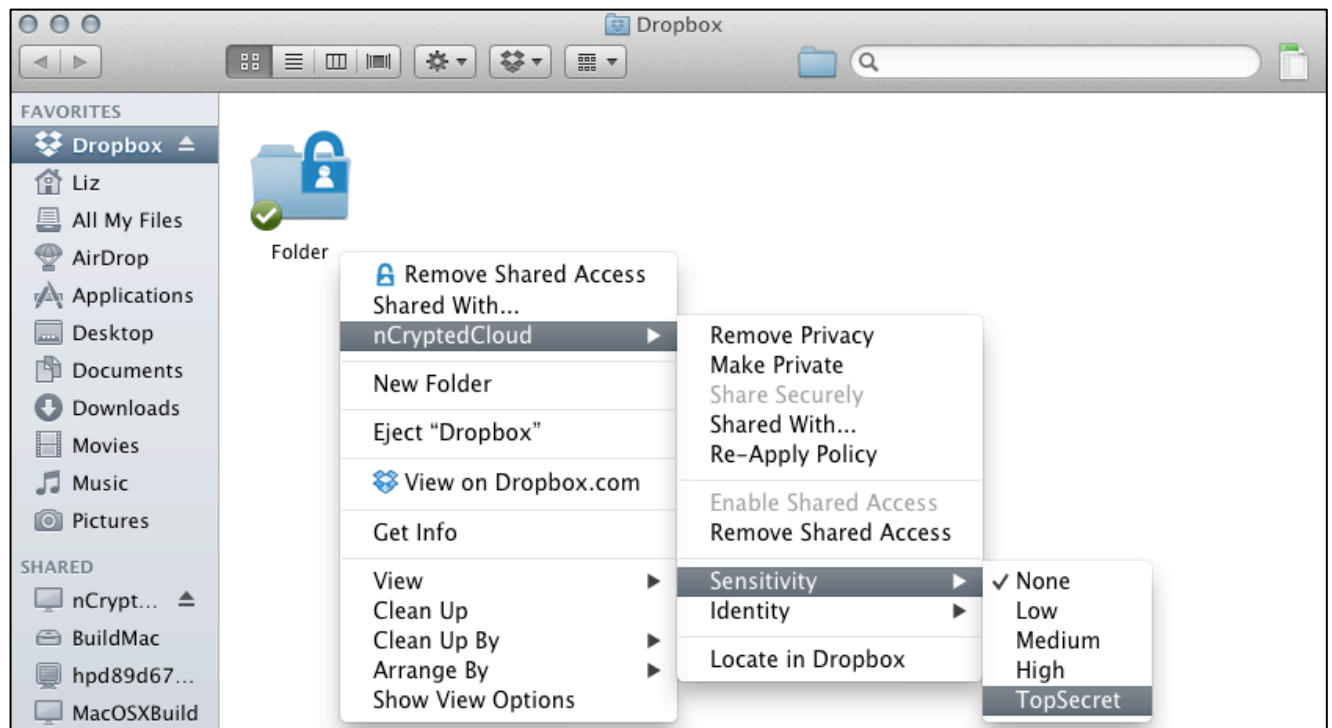
How To Apply Sensitivity

In order to apply sensitivity, you must first make sure your Advanced Settings are on.

To turn advanced settings on, right-click the nCrypteCloud Icon on you Desktop and select "Preferences", then check the "Show Advanced Features" box (line 2)

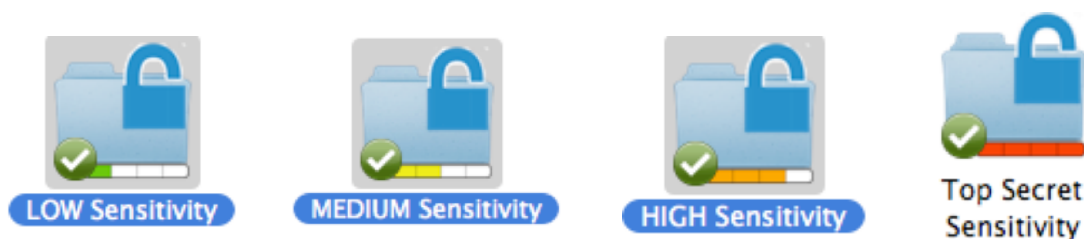


Now that your advanced settings are turned on, you can adjust your sensitivity settings.



To apply sensitivity to a folder, right-click the folder, select 'nCrypteCloud', then select 'Sensitivity'.

You will have 5 Sensitivity options: no sensitivity, Medium Sensitivity, High Sensitivity, or Top Secret Sensitivity.



The applied sensitivity settings are easily distinguishable on the folder view.

Pin Lock

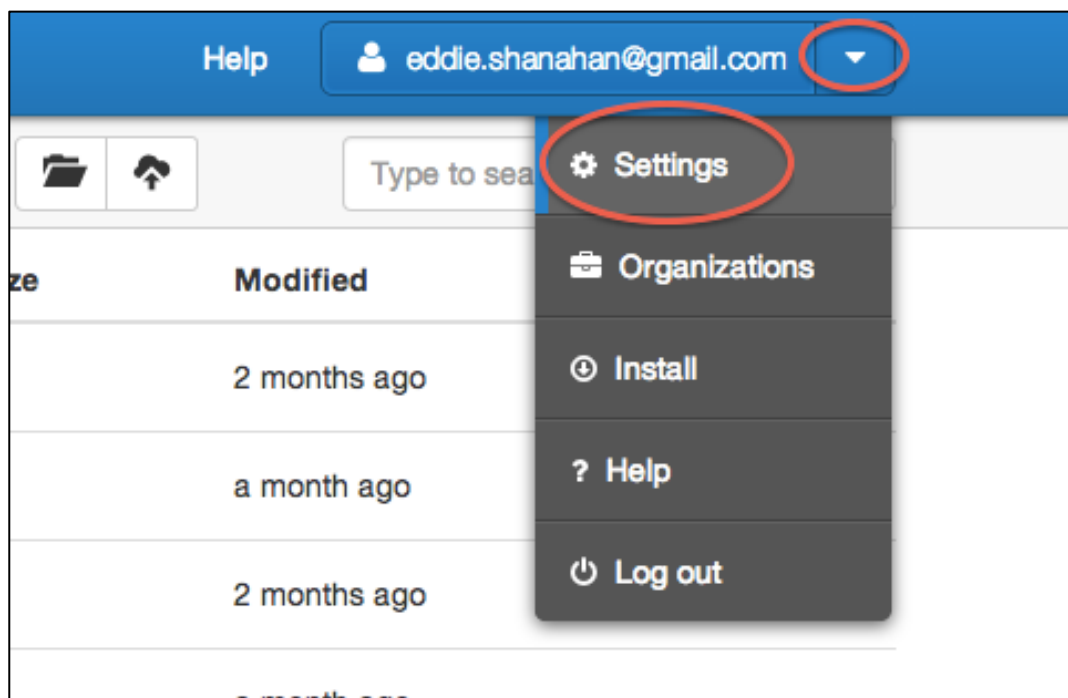
8

nCrypteCloud has implemented a Pin Lock system on the desktop client to ensure that no unauthorized users have access to your cloud data. When applied, it will prevent anyone from accessing the nCrypteCloud folder, which can be set as the default viewer for all cloud storage providers. In this way, users can implement a defense-in-depth approach to securing their data in the cloud.

*In order for the Pin Lock system to work, you need to first make sure you have set a centralized pin.

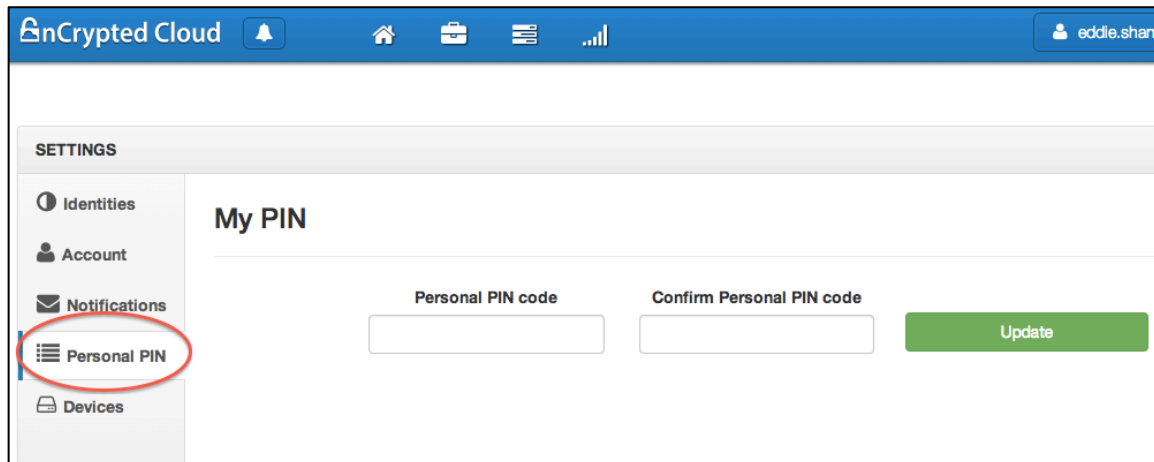
How To Set a Centralized Pin

First, log in to the nCrypteCloud Web Portal. Then, access the settings tab by clicking on the arrow to the right of your email address, and select 'Settings'.



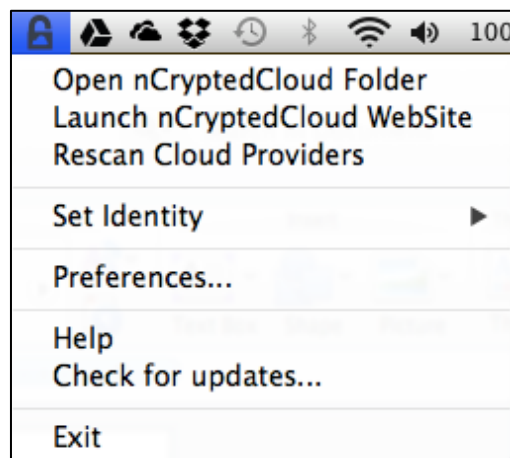
From the Settings menu, navigate down to the 'Personal Pin' tab and set a pin.

You will need to wait 5 minutes for the centralized Pin to take affect, or quit and restart the nCrypte Cloud client.

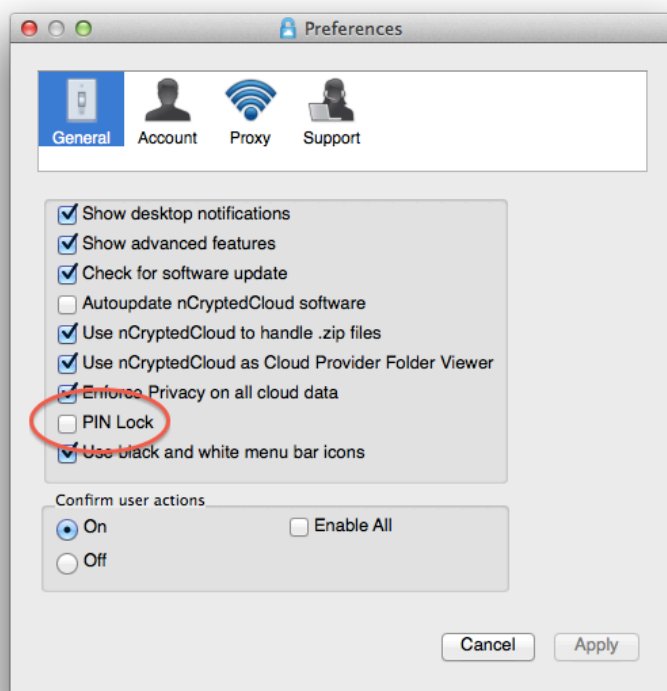


How To Enable PIN Lock on the nCrypte Cloud Client

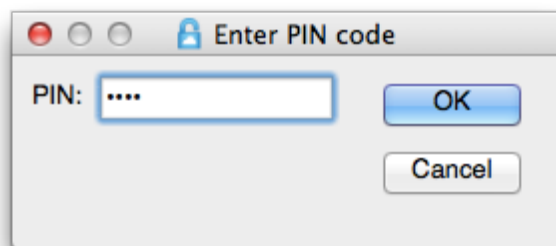
Once you have set your personal pin, click on the nCrypte Cloud lock icon in the menu bar and select 'Preferences' from the dropdown menu.



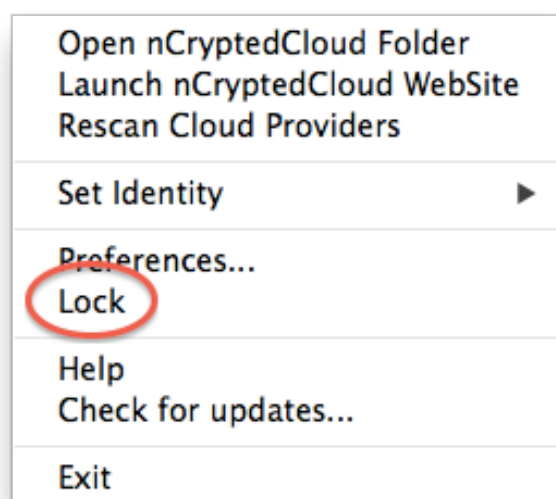
Check the box marked PIN Lock. If you have not already set your personal pin, the PIN Lock box will appear greyed out and you will be unable to select it.



An Enter PIN code menu will appear. Enter the pin you previously created through the web portal and select OK. Then Select Apply to close the preferences menu.

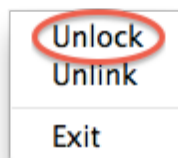


Now, when you click on the lock icon a new 'Lock' option will appear below 'Preferences'.



When selected, the 'Lock' function will prevent access to all folders/cloud hard drives within nCrypted Cloud. If you already have one open, it will immediately appear blank.

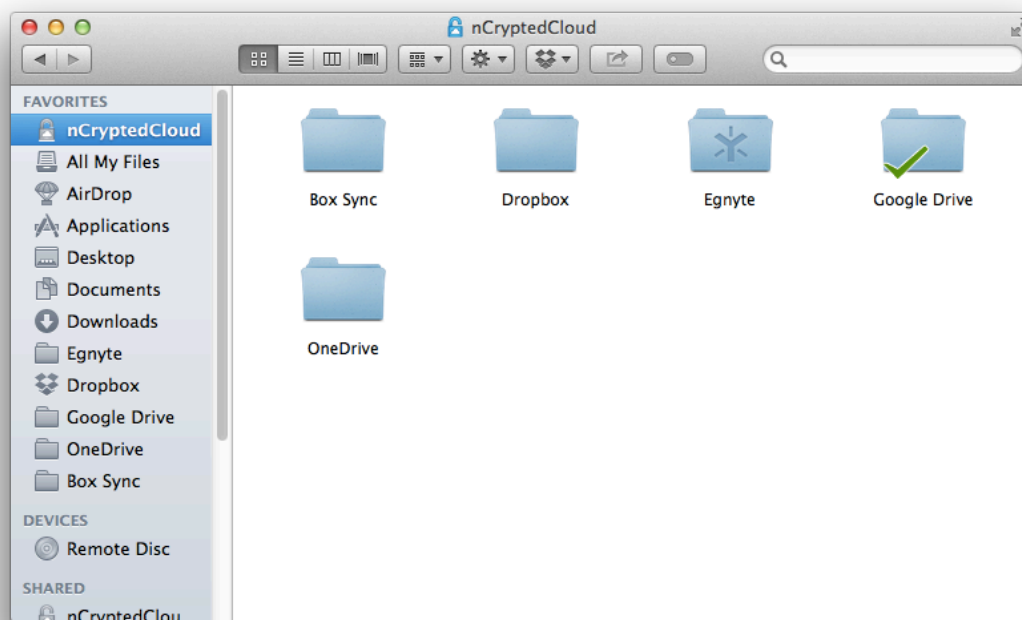
In order to disable the 'Lock' function, click on the nCrypted Cloud lock icon in the menu bar and select 'Unlock' and an enter pin window will appear. Enter your pin and select OK.



Multiple Cloud Provider/Custom Folders 9

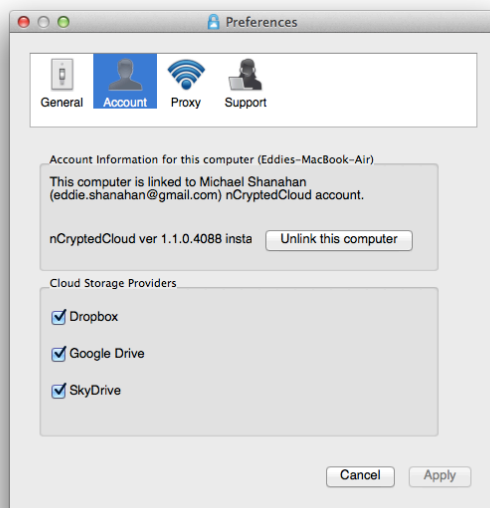
nCrypteCloud supports a number of different cloud providers, (including: Dropbox, Google Drive, OneDrive, Box, Egnyte) and provides users with an easy way to both access and apply security policies to all of their data in the cloud.

Through nCrypteCloud's virtual viewer, users are given a consolidated view of all of their cloud providers. This makes keeping track of data in multiple cloud providers as simple as possible.

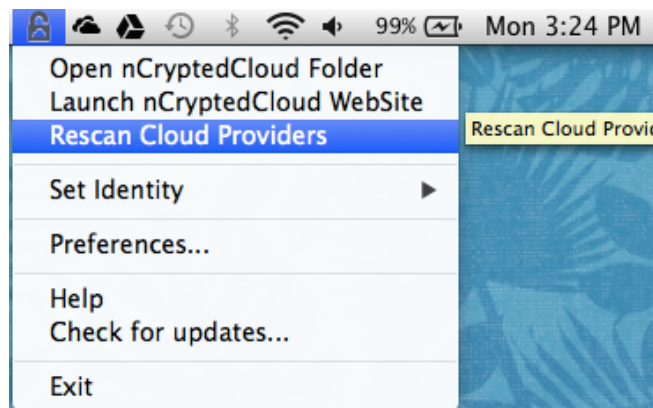


How to set up nCrypted Cloud with Google Drive and SkyDrive (OneDrive)

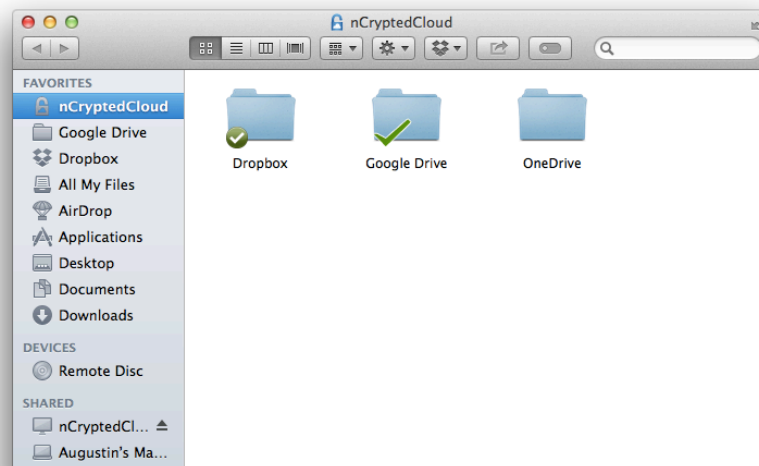
Once you have installed the latest version of nCrypted Cloud with support for Google Drive and SkyDrive (OneDrive), click on the nCrypted Cloud lock icon in the task bar and open up the **Preferences** menu. From the **account** tab, make sure the **Google Drive** and **SkyDrive** boxes are checked, and select **Apply**.



To ensure that Google Drive and SkyDrive (OneDrive) have been added to the nCrypted Cloud folder, click on the lock in your task bar and select **Rescan Cloud Providers**.



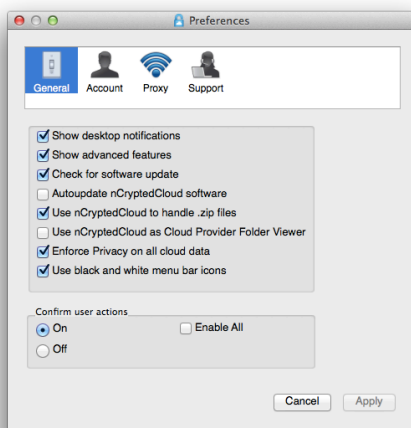
Now, when you click on the lock icon and select Open nCrypteCloud Folder, Google Drive and SkyDrive (One Drive) should appear in the Finder menu.



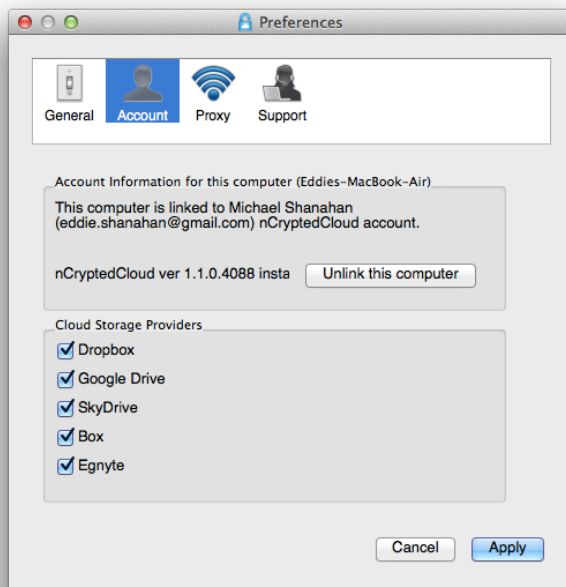
This will work whether nCrypteCloud was installed before or after the cloud service provider.

How to Set Up nCrypted Cloud with Box and Egnyte

Click on the nCrypted Cloud lock icon and select **Preferences**. From the preferences menu, check the **Show advanced features** box and select **Apply**.



Then, navigate to the **Account** tab and make sure the **Box** and **Egnyte** boxes are checked, then select **Apply**.

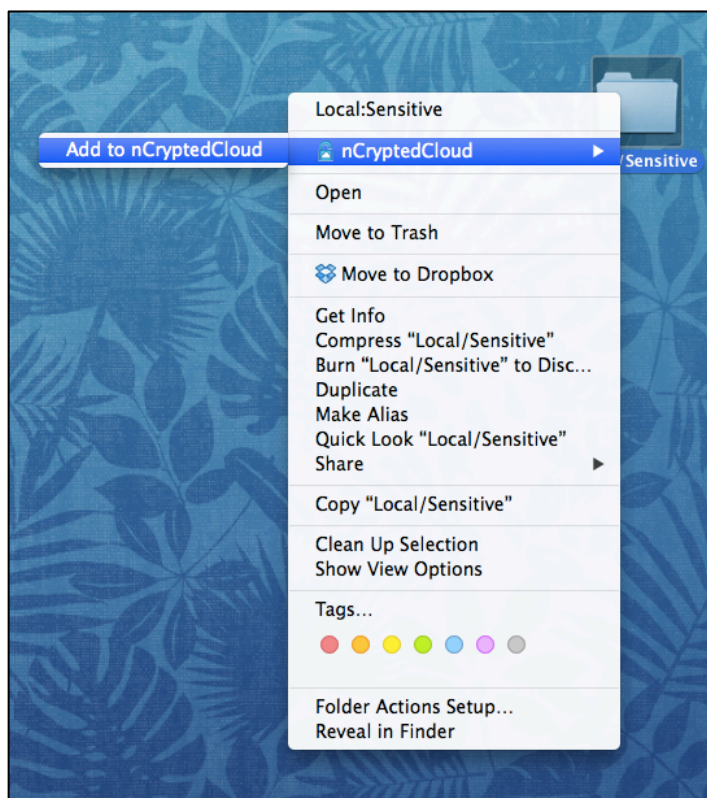


Now, when you click on the lock icon and select Open nCrypteCloud Folder, your Box and Egnyte folders should have been added to the Finder menu as well.

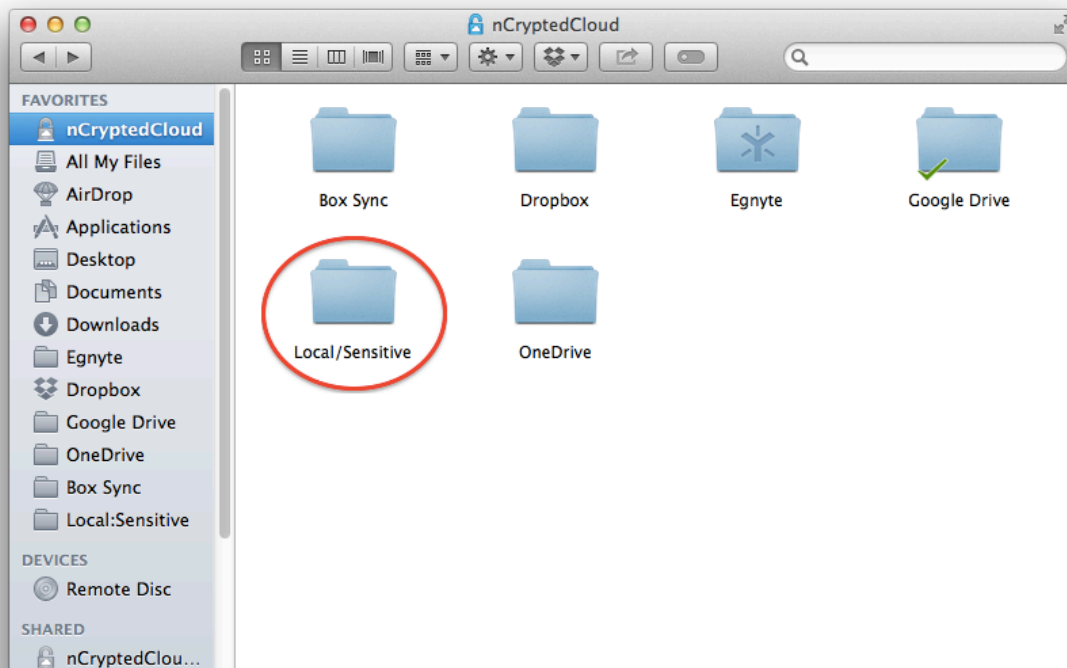
Users are also given the ability to add local directories to their nCrypteCloud folder, giving them the power to encrypt and secure any data that resides on their local hard drive.

How to add local directories to your nCrypteCloud folder

In order to add a folder from your local hard drive to nCrypteCloud, simply right click the folder, go to the nCrypteCloud menu and select "Add to nCrypteCloud".





This will automatically add the selected folder to your nCrypted Cloud viewer.



From this view, you are able to set security policies on data both locally and in the cloud.

Icon Glossary

	Private Folder
	Shared Securely
	Corporate Identity
	Low Sensitivity
	Medium Sensitivity
	High Sensitivity
	Top Secret Sensitivity